Indraprastha College for Women

University of Delhi

Course Name:	B,Sc,(Hons.) Mathematics
Paper Title:	Number Theory
Unique Paper Code:	235607
Semester:	VI
Faculty(s):	Dr. Gunjan Khurana
Year:	2023-24

Work Plan

Unit No.	Learning Objective	Lecture No.	Topics to be Covered
1	In number theory there are challenging open problems which are comprehensible at undergraduate level, this course is intended to build a micro aptitude of understanding aesthetic aspect of mathematical instructions and gear young minds to ponder upon such problems. Also, another objective is to make the students familiar with simple number theoretic techniques, to be used in data security.	1-5	Linear Diophantine equation and its solutions, Distribution of primes, Prime counting function, Statement of the prime number theorem, Goldbach conjecture.
1	Same as above	6-10	Fermat and Mersenne primes, Congruence relation and its basic properties, Linear congruence equation and its solutions.
1	Same as above	11-15	Chinese remainder theorem, to solve system of linear congruence for two variables, Fermat's little theorem, Wilson's theorem.
2	Same as above	16-25	Number theoretic functions for sum and number of divisors, Multiplicative function, and the Möbius inversion formula. The Same as above 21greatest

			integer function, Euler's phi-function.
2	Same as above	26-30	Euler's theorem, Properties of Euler’s phi-function
3	Same as above	31-40	The order of an integer modulo n2. Primitive roots for primes.
3	Same as above	41-45	Composite numbers having primitive roots.
3	Same as above	46-50	Definition of quadratic residue of an odd prime, and Euler's criterion.
4	Same as above	51-70	The Legendre symbol and its properties. Quadratic reciprocity law. Quadratic congruencies with composite moduli.: Public key encryption, RSA encryption and decryption scheme.

Syllabus		
Unit	**Contents**	**Contac t Hours**
I	Distribution of Primes and Theory of Congruencies Linear Diophantine equation, Prime counting function, Prime number theorem, Goldbach conjecture, Fermat and Mersenne primes, Congruence relation and its properties, Linear congruence and Chinese remainder theorem, Fermat's little theorem, Wilson's theorem..	15
II	Number Theoretic Functions Number theoretic functions for sum and number of divisors, Multiplicative function, Möbius inversion formula, Greatest integer function. Euler’s phi-function and properties, Euler’s theorem.	15
III	Primitive Roots The order of an integer modulo n, Primitive roots for primes, Composite numbers having primitive roots; Definition of quadratic residue of an odd prime, and Euler’s criterion.	20

IV	Quadratic Reciprocity Law and Public Key Encryption The Legendre symbol and its properties, Quadratic reciprocity, Quadratic congruencies with composite moduli; Public key encryption, RSA encryption and decryption	20
	Total	**70**

Text Books/Suggested Readings:

S. No.	**Name of Authors/Books/Publishers**	**Year of Publication/ Repr int**
1.	Burton, David M. . Elementary Number Theory (7th ed.). Mc-Graw Hill Education Pvt. Ltd. Indian Reprint.	2012
2.	Jones, G. A., & Jones, J. Mary. Elementary Number Theory. Undergraduate Mathematics Series (SUMS). First Indian Print.	2005
3.	Neville Robinns. Beginning Number Theory (2nd ed.). Narosa Publishing House Pvt. Limited, Delhi.	2007

	Paper Components		
Credits	**Lecture (L)**	**Tutorial (T)**	**Practical (P)**
	5	**1**	

Assessment Scheme

S.No.	**Component**	**Marking Scheme**	**Total Marks**
1	Internal Assessment		**25**
	● Assignment/Quiz/Project/ Presentation	10	
	● Class Test	10	
	● Attendance	5	
3.	Practical		
	● Continuous Assessment		
	● End Term Written/Practical Exam		
	● Viva		
4.	End Semester Examination		75